FISSA+ Privacy and Records Management

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W Z

0-Day Attack

Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers that are unknown to others, undisclosed to the software vendor, or for which no security remediation is available.

419 Scams

A confidence trick in which the victim is persuaded to advance the crook money in the hope of realizing larger gain. Named after the section of the Nigerian criminal code dealing with such fraud.

A back to top

Access

The ability to read, write or delete data governed by file system permissions.

Access Control Lists (ACL)

A list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. In a typical ACL, each entry in the list specifies a subject and an operation: for example, the entry (Alice, delete) on the ACL for file WXY gives Alice permission to delete file WXY.

Access Point (AP) or **Wireless Access Point** (WAP)

A device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a wired network, and can relay data between the wireless devices (such as computers or printers) and wired devices on the network. Some DOI buildings have WAP installations.

Access to Privacy Act Records

Each agency that maintains a system of records shall, upon request by any individual to gain access to his/her record or to any information pertaining to him/her which is contained in the system, permit him/her and upon his/her request, a person of his/her own choosing to accompany him/her, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him/her, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.

Accountability back to top

Ethics: The readiness or preparedness to give an explanation or justification for one's judgments, intentions, acts and omissions when appropriately called upon to do so.

Technology: the traceability of actions performed on a system to a user, process or device. For example, the unique user identification and authentication supports accountability; the use of shared user IDs and passwords inhibits accountability.

Active Content

Refers to the contents of electronic documents that can carry out or trigger actions automatically on a computer platform without the intervention of a user. Active content includes built-in macro processing, scripting languages, or virtual machines. Electronic documents with active content can have the same capability as programs when loaded into word processors. A significant share of today's malware involves active content. Examples of active content documents are Portable Document Format (PDF) documents, web pages, desktop applications containing macros, and HyperText Markup Language (HTML) encoded email bearing executable content or attachments. Examples of uses of active content are stock tickers, weather maps, online banking programs, live camera views, and programmed web broadcasts.

Active X

A framework for defining reusable software components (known as controls) that perform a particular function or a set of functions in Microsoft Windows in a way that is independent of the programming language used to implement them.

Advanced Security Operations Center (ASOC)

DOI's frontline for network security monitoring, intrusion detection and prevention, incident response and security coordination with all Bureau security programs.

Ad Hoc

A decentralized wireless network. The network is ad hoc because each node can forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to wired networks in which routers perform the task of forwarding data. It is also in contrast to managed (infrastructure) wireless networks, in which a special node known as an access point manages communication among other nodes.

Adware

Software that allows banner ads or pop-up ads to display on your computer. It downloads to your computer when you access certain sites on the Internet, or when you agree to download it when you use certain freeware or shareware. Some adware will also track your files, track where you surf on the Internet, and then report back to advertisers to help them direct particular ads to you.

Anti-Malware back to top

Programs that combat malware in two ways. 1.) They can provide real-time protection against the installation of malware software on a computer. This type of spyware protection works the same way as that of anti-virus protection in that the anti-malware software scans all incoming network data for malware software and blocks any threats it comes across. 2.) Anti-malware software programs can be used for detection and removal of malware software that has already been installed onto a computer. This type of malware protection is normally much easier to use and more popular. This type of anti-malware software scans the contents of the windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found, allowing the user to choose which files to delete or keep, or to compare this list to a list of known malware components, removing files that match.

Assistant Director for Information Resources (ADIR)

Replaces position(s) formerly titled as CIO within DOI bureaus and Subordinate Organizations. ADIRs serve two year term appointments unless otherwise authorized by the DOI CIO and the Executive Resources Board, and report to bureau heads.

Attended Fax
An attended fax is a means by which an employee can safely transmit PII across distances. To carry out an attended fax, first ensure you have the correct fax number. Then telephone the recipient and make sure that person is standing by to receive the fax. Submit the fax, then double-check to ensure in the fax confirmation that it went to the correct number and that all pages were successfully sent.

Audits
An examination of the controls within an Information Technology (IT) infrastructure. An IT audit is the process of collecting and evaluating evidence of an organization's information systems practices and operations. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively and efficiently to achieve the organization's goals or objectives.

Authentication

A process of proving the identity of a computer or computer user, commonly with a username and password or PIV card.

Authorization

A process of determining what types of access are permitted. Data owners authorize users to access files or folders; giving someone your password authorizes them to perform actions under your login that you may not know about.

Availability

One of the three goals (Confidentiality, Integrity, Availability) of a secure information system. Availability is defined as ensuring timely and reliable access to and use of information to authorized users.

B back to top

Backups

Making copies of data so that these additional copies may be used to *restore* the original after a data loss event. These additional copies are typically called "backups." Backups are useful primarily for two purposes. The first is to restore a state following a disaster (called disaster recovery). The second is to restore small numbers of files after they have been accidentally deleted or corrupted.

Business Impact Assessment (BIA)

An impact analysis that results in the differentiation between critical and non-critical organizational functions/activities. A function is considered critical if the organization cannot fulfill its mission without it, or if dictated by law. For each critical function, two values are then assigned:

- Recovery Point Objective (RPO) - the acceptable latency of data that will be recovered
- Recovery Time Objective (RTO) - the acceptable amount of time to restore the function

The impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the business and technical requirements for recovery of the critical function.

Bit-Torrent

A peer-to-peer file sharing (P2P) communications protocol.

Bluetooth

An open wireless protocol for exchanging data over short distances from fixed and mobile devices, creating personal area networks (PANs).

Bot herder

An attacker who controls a bot-net.

Bot-net (ro**bot net**work) **or Botnet** is a jargon term for a collection of software robots, or bots, that run autonomously and automatically. The term is often associated with malicious software but it can also refer to the network of computers using distributed computing software. While the term "botnet" can be used to refer to any group of bots, such as IRC bots, this word is generally used to refer to a collection of compromised computers (called Zombie computers) running software, usually installed via worms, Trojan horses, or backdoors, under a common command-and-control infrastructure. Bot-network operators are hackers; but instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam and malware attacks, or hiding their tracks through connections with multiple systems when illegally accessing other important or secure networks. The services of these bot-networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).

Breach

A breach is an actual or suspected, real or potential, occurrence of unauthorized disclosure or access of information. Such an occurrence triggers responsibilities on the part of employees including immediate notification of appropriate personnel.

Browser – a generic term used to refer to software that lets individuals view pages from various sources including Web servers on the Internet. Internet Explorer and Firefox are two popular browsers that aid in navigating text, graphics hyperlinks, audio video and other multimedia information and web services. Components can be installed in the browser to give it additional functions. Often the extensions require full access to the browser internals and underlying operating system. Malware using those extensions can be used to compromise the entire computer.

Browser attack

A general term referring to any number of attacks that can be accomplished through web browsers. Browser attacks include 'Man-in-the-Browser', cross-site cooking, HTTP cookie, cross site scripting, spyware, JavaScript, and cross zone scripting.

Bureau

A bureau is any constituent component of the Department. The Office of the Secretary (which includes all of the Departmental offices as well as other offices), the Office of the Solicitor, and the Office of the Inspector General are also considered as bureaus.

Bureau Chief Information Security Officer (BCISO)

[Formerly Bureau Information Technology Security Manager (BITSM)]

With the promulgation of the DOI IT Security Policy Handbook, the BITSM title has been replaced with Bureau Chief Information Security Officer (BCISO).

Bureau/Office FOIA Officer

The person within a bureau or office who administers the Freedom of Information Act with that bureau or office, under the overall guidance of the Departmental FOIA Officer. This includes acknowledging and responding to FOIA requests to the bureau or office, applying exemptions, and participating in FOIA reporting requirements on behalf of the bureau or office.

Bureau/Office Information Collection Clearance Officer

The person within a bureau or office who administers the Paperwork Reduction Act for that bureau or office, including working with program offices to develop the proper notices and Supporting Statement for new and existing information collections under the Paperwork Reduction Act.

Bureau/Office Privacy Officer/Privacy Act officer

The person within a bureau or office who administers the Privacy Officer/Privacy Act Officer functions of a bureau or office, under the overall guidance of the Departmental Privacy Officer. This includes working with program offices to develop and revise system of records notices, privacy impact assessments, fulfill privacy reporting requirements on behalf of the bureau or office, serve as a consultant and guide within the bureau or office on privacy matters, conduct privacy reviews under OMB guidance, and participate in breach response and remediation for bureau or office related breaches.

C back to top

Computer Emergency Readiness Team / Coordinator Center

Acronym for the CERT® Coordination Center - CERT/CC is a center of Internet security expertise, established in 1988, located at the Software Engineering Institute, and a federally-funded research and development center operated by Carnegie Mellon University.

Cell Phones

Cell phones are basically radio transmitters. Anyone with the right equipment can listen to conversations. Use a land line for more privacy, and never discuss sensitive information on an unsecured phone.

Certificate (see also digital certificate)

Digital files that are provided by a central “certificate authority” to give assurances of identity. They verify that a given public key belongs to a given individual or corporation.

Chain letter

An e-mail message that induces a recipient to pass the e-mail on to as many other recipients as possible. Common methods used in chain letters include emotionally manipulative stories, get-rich-quick pyramid schemes, and the exploitation of superstition to threaten the recipient with bad luck, or worse, if the chain is broken or the conditions in the message are not followed. In the US, chain letters that request money or other valuables and promise a substantial return is considered a form of gambling and therefore is illegal. Other types of chain letters are viewed as a nuisance.

Chief Information Officer (CIO)

The Department has an overall Chief Information Officer who also serves, at DOI, as the SAOP (Senior Agency Official for Privacy).

Chief Information Security Officer (CISO)

The DOI staff member charged with overseeing the security of the department’s information systems and resources. The CISO focuses on information security coordination, policy, and compliance throughout the department.

Chief Technology Officer (CTO) back to top

The person responsible for planning the direction of technology in a bureau. The department also has a designated CTO.

Circular

Directives issued by the Office of Management and Budget (OMB).

Civil Action

Any lawsuit relating to civil matters and not criminal prosecution.

Civil Liberties

Fundamental individual rights such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments—to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights

Rights and privileges of citizenship and equal protection that the state is constitutionally bound to guarantee all citizens regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Protection of civil rights imposes an affirmative obligation upon government to promote equal protection under the law. These civil rights to personal liberty are guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term civil rights involves positive (or affirmative) government action to protect against infringement, while the term civil liberties involves restrictions on government.

Client Computing

Term used in reference to a multitude of computers that each individually may access resources on a central computer and then have it displayed on one or more of the multitude of computers. Web browsers, for example, run on client computers by downloading and displaying (or rendering) content from the central web server. Citrix is another example of client computing. Citrix client software accesses the Citrix server which passes a screen image back to the client computer while doing all the actual processing on the Citrix server(s).

Cloud Computing

A style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Email services are frequently identified as potential cloud computing applications.

Code back to top

A somewhat informal reference to computer programming code or scripting commands.

Code of Federal Regulations

The Code of Federal Regulations (CFR) is the codification of the general and permanent rules published in the Federal Register by the executive departments and agencies of the federal government.

Command and Control Server (C&C)

A computer used by a bot-herder to control the zombies on a bot-net.

Computer Incident Response Center (CIRC)

An entity that provides an organization with computer security related incident response capabilities. The DOI CIRC coordinates threat identification and incident remediation with US CERT. At DOI, it is an integral part of the Advanced Security Operations Center (ASOC).

Confidentiality

One of the three goals (Confidentiality, Integrity, Availability) of a secure information system. Confidentiality is defined as preserving authorized restrictions on access and disclosure, including means for protecting sensitive or classified information.

Contingency Plan (CP)

Specific strategies and actions to deal with a particular problem, emergency or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are designed to help governments, businesses or individuals to recover from incidents in the minimum time with minimal cost and disruption.

Controlled Unclassified Information (CUI)

A new category of unclassified categories issued in a directive on May 9, 2008 by President George W. Bush. CUI is intended to facilitate the sharing of sensitive information between organizations and replace categories such as For Official Use Only (FOUO), Sensitive But Unclassified (SBU) and Law Enforcement Sensitive (LES) categories.

Cookies

Short text files that websites write to a temporary folder on a client computer. They often contain sensitive information and can contain password(s), name, or any other information entered on a website. A website can retrieve a cookie it placed there or cookies from other websites. There are programs that "mine" cookies. These programs can be used to track sites visited on the Internet and then collect information pertinent to the sites (e.g., your bank account number and PIN). Browsers can be set to block cookies and issue prompts on how to handle them as needed.

Copyright laws back to top

Copyright laws protect the right of an author to control the public distribution, reproduction, display, and adaptation of his/her original work.

Corruption, fraud, waste, and abuse

Corruption occurs when the opportunity exists and when oversight is lacking. Fraud is a criminal action; waste and abuse are ethical lapses. If you observe corruption, fraud, waste, or abuse, under the Whistleblower Act, you have a responsibility to report it according to your appropriate Bureau/Office procedure.

Crimeware

Malicious software (Trojans, key loggers) that specifically targets financial transactions, especially electronic funds transfers, and are designed to circumvent security authentication mechanisms, and initiate fraudulent wire transfers and take over financial accounts.

Criminal Groups

Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, techniques, bot-nets and spyware/malware to commit crime, including identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage, large-scale monetary theft and to hire or develop hacker talent.

Critical infrastructure

Critical infrastructure provides the essential services that underpin American society. They are the physical structures and computer-based systems essential to the operations of the economy and government. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause mass casualties, catastrophic health or economic effects comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both government and private. Many of the Nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. However, they have become increasingly automated and interlinked, creating new vulnerabilities to equipment failures, human error, weather and other natural causes, physical and cyber attacks.

Cryptographic system

A system for converting information from its normal, comprehensible form into a form that is unreadable without special knowledge (encryption). A system that is designed to protect confidentiality and integrity against hostile attack.

CUI (Controlled Unclassified Information)

Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. The CUI designation replaces "Sensitive But Unclassified (SBU), For Official Use Only (FOUO), Law Enforcement Sensitive (LES), LIMITED DISTRIBUTION" and other similar control markings.

Cyber Attack

The use of computer vulnerabilities to conducting attacks against individual computers or organizational networks over the Internet or other computer networks.

Cyber Threat

The agents by which an individual's computer or an organization's computer network might be compromised. Foreign governments trying to conduct espionage may be a cyber threat, criminal groups may be cyber threats; accidental loss of data by an individual is also a cyber threat.

Cyber Warfare

Programs by national governments are unique in posing a threat along a wide spectrum of objectives that might harm US interests. Russia's cyber attack on Estonia for political reasons in 2007 was the first well documented example of cyber warfare. The goal of cyber warfare is to weaken, disrupt or destroy communication networks, to confuse and to inhibit prompt reaction. The sub-goals include espionage for attack purposes, espionage for technology advancement, disruption of infrastructure to attack an economy, or could be a full scale attack on infrastructure in response to a first strike.

D back to top

Data

A collection of facts from which conclusions may be drawn; statistical data.

Defense-In-Depth

The concept of putting in many layers of security so that if one fails others succeed.

Denial of Service (DoS)

Result of any action or series of actions that prevents any part of an information system from functioning. On the Internet, a DoS attack is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. From the NIST 800-61 Incident Response DoS is an incident in which

- An attacker sends specially crafted packets to a Web server, causing it to crash.
- An attacker directs hundreds of external compromised workstations to send as many Internet Control Message Protocol (ICMP) requests as possible to the organization's network.

Departmental Privacy Officer back to top

The Departmental Privacy Officer is the person within the OCIO designated to have the leadership of the privacy activities for the Department. This includes promulgation of privacy policies and procedures, oversight of bureau privacy programs, coordination of all privacy activities, and preparation of privacy reports to external entities with bureau or office assistance.

Digital Certificate (see Certificate)

DI-3710 Disclosure Accounting Form

Official DOI form used to record the date, nature and purpose of each disclosure from a Privacy Act systems of records, and the name and address of the individual or agency to whom the disclosure is made (See the Privacy Act, 5 U.S.C. 552a (c) for requirements to account for records disclosed to external parties).

Disclosure

Disclosure means release of information contained in a system of records to any person (other than the person to whom the information pertains), including any employee of the Department of the Interior and employees of other federal departments and agencies.

Disposition

The actions taken regarding records no longer needed for current government business. For example, (1) transfer to agency storage facilities or federal records centers, (2) transfer from one federal agency to another, (3) transfer of permanent records to the National Archives, and (4) disposal of temporary records.

Distributed Denial of Service (DDoS)

A type of DoS attack in which an attacker uses malicious code installed on various computers or a bot net to attack a single target.

DM

Departmental Manual. The written policy decisions of each cabinet level department.

DMZ

Demilitarized Zone, also known as a Data Management Zone**,** Demarcation Zone or Perimeter Network, is a physical or logical subnetwork that contains and exposes an organization's external services to an untrusted network, such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's network; the public has access only the system in the DMZ, rather than the whole of the network.

Documentary materials back to top

A collection term for records, non-record materials, and personal papers that refers to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording.

DOI CIRC (DOI Computer Incident Response Center)

DOI's central reporting organization for computer incident response and tracking. All DOI incidents must be reported through the BCISO to DOI CIRC, who tracks them and may report them to US-CERT.

DOI Privacy Act Regulations

The legal requirements derived by the elements addressed in the Privacy Act as applied to the Department of the Interior.

Due Care

The care that a reasonable man would exercise under the circumstances; the standard for determining legal duty.

Due Diligence

The term used for a number of concepts involving either the performance of an investigation of a business or person, or the performance of an act with a certain standard of care. It can be a legal obligation, but the term will more commonly apply to voluntary investigations.

"Due diligence" first came into common use as a result of the United States' Securities Act of 1933. The US Securities Act included a defense referred to in the Act as the "Due Diligence" defense which could be used by broker-dealers when accused of inadequate disclosure to investors of material information with respect to the purchase of securities. As long as they disclosed to the investor what they found, they would not be held liable for nondisclosure of information that was not discovered in the process of that investigation.

Dumpster Diving

The practice of sifting through commercial or residential trash to find items that have been discarded by their owners, but which may be useful to the dumpster diver.

E back to top

E-Government Act of 2002

The E-Government Act of 2002 was created to enhance the management and promotion of electronic government services and processes by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to government information and services. Regarding privacy, it instituted the requirement for federal agencies to conduct Privacy Impact Assessments for all electronic systems with PII of the public.

Encryption

The process of encoding electronic information to allow secure transmission of data over the Internet. WEP, WPA and WPA2 are encryption standards for wireless networks. PGP and GPG are examples of file encryption products.

Enterprise Services Network (ESN)

The DOI-wide Wide Area Network (WAN) that connects all DOI bureaus to each other and the internet. The ESN includes five security gateways that all traffic coming to or from the internet traverses. The ESN and all of its network and security devices are outsourced and managed by Verizon.

Extensions

Browsers were intended to be simple readers and renderers of HTML. To add functionality to what browsers can do, programs were written to allow graphics, video, audio or other rendering capability to be done through the browser. These programs or extensions “extended” the capability of browsers.

EULA (End User License Agreement)

A legal contract between the author and the user of an application. The EULA, usually referred to as the "software license”, is a certain form of an agreement. The user may agree to pay for the opportunity of using the software, and promises the software manufacturer to follow the rules provided in the EULA.

F back to top

Fax Machines

In most circumstances, there is no control over who receives information transmitted over a fax machine. Verify that the recipient will be there to pick up the fax immediately if sending sensitive information.

FDCC (Federal Desktop Core Configuration)

A program, coordinated by NIST in conjunction with DoD and DHS, to improve information security by deploying a standard secure configuration on computers that utilize the Microsoft Windows XP or Vista operating systems throughout the federal government. Federal agencies with these operating systems must adopt the standard security configurations by February 1, 2008. (See also USGCB).

Federal Information Security Management Act of 2002 (FISMA)

The Federal Information Security Management Act was enacted as Title III of the E-Government Act. It establishes numerous reporting requirements for federal agencies to measure compliance with various provisions of federal privacy law, especially addressing electronic records.

Federal Information System Security Awareness (FISSA)

Annual security awareness training required for all users of federal systems by the Federal Information Security Management Act of 2002 and numerous Office of Management and Budget memoranda.

Federal Records

Federal records are documentary materials created or received in the transaction of government business, regardless of media.

Federal Records Act

The Federal Records Act of 1950, as amended, establishes the framework for records management programs in federal agencies.

Federal Register

The Federal Register is the official government daily publication for rules, proposed rules, and notices of federal agencies and organizations, as well as executive orders and other presidential documents. Privacy Act System of Records Notices, for example, are published in the Federal Register, as are notices associated with Paperwork Reduction Act compliance.

File plan back to top

A file plan lists all of the records created by a bureau or office Records Officer, or program staff, and maintained by an employee, contractor or staff member of that bureau or office. The office file plan should be applied to records in all media (e.g. paper, non-paper, and electronic).

Firewall

A part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is an application, device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.

Firmware

Software stored in read-only memory (ROM) or programmable ROM (PROM). It is often responsible for the behavior of a system when it is first powered on. A typical example would be a "monitor" program in a microcomputer that loads the full operating system from disk or from a network and then passes control to it.

Flash

Adobe Flash (formerly Macromedia Flash) is a method of adding animation and interactivity to web pages and to develop rich Internet applications. Flash can manipulate vector and raster graphics and supports bidirectional streaming of audio and video.

Fraud

Any intentional deception designed to deprive the United States unlawfully of something of value or to secure something from the US a benefit, privilege, allowance or consideration to which an individual is not entitled. Such practices include, but are not limited to, the offer, payment or acceptance of bribes or gratuities; making false statements; submitting false claims; using false weights or measures; evading or corrupting material fact, adulterating or substituting materials, falsifying records and account books, arranging for secret profits, kickbacks or commissions; and conspiring to use any of these devices. The term also includes conflict of interest cases, criminal irregularities, and the unauthorized disclosure of official information relating to procurement and disposal matters.

Freedom of Information Act of 1966 (FOIA)
An Act designed to provide agency records upon request unless certain exemptions apply to all or part of the records. Refer to DOI FOIA regulations for more information about processing information under the FOIA that originated from the Privacy Act System of Records.

Freeware

Computer software that is available for use at no cost or for an optional fee. Freeware can be proprietary software available at zero price. The author usually restricts one or more rights to copy, distribute, and make derivative works of the software.

FOUO

For Official Use Only. A type of sensitive information that falls into the category of Controlled Unclassified Information (CUI).

G back to top

Government Furnished Equipment (GFE)

Computer equipment that is bought with government funds for the use by government employees.

General Support System (GSS)

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. (From OMB Circular A-130 Appendix III.)

H back to top

Hackers

Individuals who break into networks for the thrill of the challenge or for bragging rights in the hacker community. However, according to the Central Intelligence Agency, most hackers do not have the requisite expertise to threaten difficult targets such as critical US networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.

Hactivism and Terrorists

The expansion of the Internet has opened the door to dangerous new classes of political threats. As Internet access increases exponentially around the world, **"**hacktivists**",** or hacker activists, may hold virtual sit-ins, visiting a site en masse to shut it down. They can cause a "denial of service" by deluging an inbox with an "e-mail bomb". Hacktivists may also deface web pages or post messages of political protest.

Information security experts fear that cyber terrorists may use similar tactics to attack the critical infrastructure of the United States, causing anything from economic instability to the loss of human life. Because of high visibility and name recognition throughout the world, United States government, cultural, or corporate networks are particularly vulnerable to attack. Furthermore, perceived positions on certain issues or support of certain groups may make these sites targets in conflicts that do not even directly concern them.

Hardware Development Life Cycle (HDLC) (See System Development Life Cycle)

Hash or Hashing back to top

Hashing is producing *hash values* for detecting accidental or intentional changes to the data. A hash value (or simply *hash*), also called a *message digest*, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact. Common hashing algorithms are MD5 or SHA.

Hash Checker

A program that recalculates the hash of a file for comparison with a given hash. For example a hash string may be provided with a file to be downloaded. After downloading the file run the hash checker.

Homeland Security Information

Any information possessed by a state, local, Tribal, or federal agency that relates to a threat of terrorist activity or to the ability to prevent, interdict, or disrupt terrorist activity, or would improve the identification or investigation of a suspected terrorist or terrorist organization or the response to a terrorist act.

HSPD-12 Homeland Security Policy Directive -12

Establishes a framework for identifying individuals and mandates use of two factor authentication for federal agencies.

Hyper Text Transfer Protocol (HTTP)

An application-level protocol for distributed, collaborative, hypermedia information systems. Its use for retrieving inter-linked resources led to the establishment of the World Wide Web.

Hyper Text Transfer Protocol Secure (HTTPS)

A computer protocol that encrypts and decrypts user page requests as well as the pages returned by the web server. The use of HTTPS protects against eavesdropping and man-in-the-middle hijacking attempts, and requires a certificate from the server to verify the authenticity of the server in the transaction. As an example, suppose you visit a retailer's Web site to view their online catalog. When you're ready to order, you will be given a Web page order form with a Uniform Resource Locator (URL) that starts with https://. When you click "Send," to send the page back to the catalog retailer, your browser's HTTPS layer will encrypt it. The acknowledgement you receive from the server will also travel in encrypted form, arrive with an https:// URL, and be decrypted for you by your browser's HTTPS sublayer.

I back to top

Identity Theft

Use of another's personal information to commit fraud. Financial information, medical information, social security number, address, phone are all used. Crimes such as purchasing items under another person's credit, and receiving medical services under another person's insurance, transferring money from the owner's financial accounts all constitute criminal acts. Occurrences of identity theft are dramatically increasing.

IM (Instant messaging)

A form of real-time communication between two or more people based on typed text. The text is conveyed via devices connected over a network, such as the Internet.

Inappropriate Usage

The following are a few examples of *Inappropriate Usage***.** A user provides illegal copies of software to others through peer-to-peer file sharing services. A person threatens another person through email.

Indian Fiduciary Trust records

Documents used in the management of Indian trust assets such as land, natural resources, and monies held in trust by the federal government for individual Indians, Indian tribes, or Alaska natives and Alaska native organizations. The Department retains them permanently.

Incident

Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of service. Incident management, therefore, is basically the process of restoring operations as quickly as possible with minimal adverse impact on business operations. (See Denial of Service, Inappropriate Usage, Malicious Code, Unauthorized Access.)

Individual

For purposes of the Privacy Act, an individual means a citizen of the United States or an alien lawfully admitted for permanent residence.

Information

A collection of related data; knowledge about a topic. Data that have been processed into a format that is understandable by its intended audience.

Information Collection Clearance Officer

The Information Collection Clearance Officer (ICCO) is responsible for establishing procedures for the systematic review of existing and proposed information collection requirements, including any requirements which would be imposed by any legislative proposals initiated by the Department and/or bureau. (See Paperwork Reduction Act.)

Information in Identifiable Form (IIF) back to top

Similar to PII, Information in Identifiable Form (or Identifiable Form) - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, (i.e., indirect identification). (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Information Sharing Environment (ISE)

A framework that enables responsible terrorism-related information sharing between and among people, projects, systems and agencies.

Informational value

The usefulness of records in documenting the persons, places, things, or matters dealt with by an agency, in contrast to documenting the agency's organization, functions, and activities. The value of information generally decreases with age.

InfoSec (Information Security)

The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.

Integrity

One of the three goals (Confidentiality, Integrity, Availability) of a secure information system. Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

The Intelligence Reform and Terrorism Prevention Act of 2004 restructured the U.S. Government's intelligence community by coordinating and integrating activities among law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel in an effort to enhance the way we detect and respond to threats. The IRTPA also established the Information Sharing Environment to ensure access to and improve the coordination, integration, sharing, and use of terrorism and homeland security information between and among Federal, state, local, tribal, and territorial agencies, the private-sector, and foreign partners.

IG or OIG (Inspector General or Office of Inspector General)

An office created for federal agencies by the Inspector General Act of 1978. Sixty four federal IGs are appointed for life to investigate matters of corruption, waste, fraud (criminal), abuse (policy violation), mismanagement and inefficiency.

IP (Internet Protocol) **address** back to top

A numeric address given to servers and users connected to the Internet of the form ###.###.###.### (IP version 4). Internet Protocol version 6 (IPv6) is designed to succeed the Internet Protocol version 4 (IPv4) with an expanded address space and other features.

IRC (Internet Relay Chat)

A form of real-time Internet text messaging (chat) or synchronous conferencing.

ISE Privacy Guidelines

The ISE Privacy Guidelines required Federal agencies to establish a robust terrorism0related information protection framework for privacy, civil rights and civil liberties. Federal agencies implement the ISE Privacy Guidelines by promulgating and implementing ISE privacy and civil liberties policies, providing training, collaborating with stakeholders and privacy and civil liberties groups to foster transparency and trust, and ensuring that privacy, civil rights, and civil liberties protections are appropriately integrated into processes, systems and information sharing agreements to maintain the information privacy and other legal rights of Americans.

ISP (Internet service provider)

A company that provides Internet access and may provide other Internet services such as e-mail or web hosting.

J back to top

Java

Java is an object-oriented language similar to C++, but simplified to eliminate language features that cause common programming errors. Java source code files (files with a *.java* extension) are compiled into a format called *bytecode* (files with a *.class* extension), which can then be executed by a Java interpreter. Compiled Java code can run on most computers because Java interpreters and runtime environments, known as *Java Virtual Machines (VMs),* exist for most operating systems, including UNIX, the Macintosh OS, and Windows. Bytecode can also be converted directly into machine language instructions by a just-in-time compiler (JIT).

JavaScript

A scripting language developed by Netscape to enable Web authors to design interactive sites. Although it shares many of the features and structures of the full Java language, it was developed independently. JavaScript can interact with HTML source code, enabling Web authors to spice up their sites with dynamic content. JavaScript is endorsed by a number of software companies and is an open language that anyone can use without purchasing a license. It is supported by recent browsers from Netscape and Microsoft, though Internet Explorer supports only a subset, which Microsoft calls *Jscript*.

K back to top

Key

A cryptographic key is used to encrypt a message (to make unreadable) and then to decrypt the same message (to make readable again).

Keystroke Logger (also key logger)

A computer surveillance tool, either software or hardware, that captures each keystroke a user types. It is usually hidden from the user and may use cloaking technology (rootkit) to hide from other software to evade detection. Key loggers may be installed by trojans with other malicious software through exploits, and are often used by online criminal gangs to facilitate identity theft and bank fraud operations.

L back to top

Laptops

The convenience and portability of laptops makes them vulnerable to theft or security breaches. Password-protect the logon to your laptop. Encrypt the hard drive of your laptop. Be careful what you display on your screen, especially in close quarters such as airplanes. Stay within arm's reach of your laptop when traveling to prevent theft. Use a cable lock in public places to prevent someone quickly grabbing your laptop.

Law Enforcement Information

Any information obtained by or of interest to a law enforcement agency or official that is both:

- Related to terrorism or the security of our homeland, and
- Relevant to a law enforcement mission, including, but not limited to:
    - Information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation;
    - Assessment of or response to criminal threats and vulnerabilities;
    - The existence, organization, capabilities, plans, intention, vulnerabilities, means, method, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct;
    - The existence, identification, detection, prevention, interdiction, disruption of, or response to criminal acts and violations of the law;
    - Identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and
    - Victim/witness assistance.

Leetspeak back to top

Leet or **Eleet** (sometimes rendered **l33t**, **1337**, or **31337**), a hacker term referring to an alphabet used primarily on the Internet, which uses various combinations of ASCII characters to replace Latinate letters. The term is derived from the word "elite", and the usage it describes is a specialized form of symbolic writing. Leet may also be considered a substitution cipher, albeit with much variation from user to user.

Lessons Learned https://www.llis.dhs.gov/index.do

A part of the incident response and disaster recovery process in which the incident is reviewed, what worked and what did not is evaluated, root cause analyses are performed and procedural changes are made to improve response to future incidents.

Litigation hold

A legal notification from the Department or Office of the Solicitor directing employees to preserve any documentary materials that may be relevant to a pending or foreseeable lawsuit or administrative adjudication.

Local Shares

A method of granting access to files or folders on a hard drive so that anyone on the same network can access the data. Granting share access is a form of peer-to-peer (P2P) communication.

Logic bomb

A logic bomb can release a virus, worm, or other code used to attack the system. It executes when a specific event occurs, such as when a certain date arrives. A logic bomb can perform a variety of malicious tasks.

M back to top

Madware

Apps that use aggressive ad libraries. Ad libraries have the ability to collect information about the app's user in order to serve targeted advertisements. Depending on which ad library features the developer chooses to use, personal data can be leaked through an ad library. Additionally, an ad library can exhibit annoying behaviors such as displaying ads in the notification bar, creating ad icons, or changing Web browser bookmarks.

Maintain

The term *maintain* includes maintain, collect, use or disseminate activities. In fact, it can apply to any possible action, including storage, of information.

Malicious code (see Malware below) back to top

Malware (Malicious Soft**ware)**

Software or firmware capable of performing an unauthorized function on an information system. It is designed with a malicious intent to deny, destroy, modify, or impede systems configuration, programs, data files, or routines. Malware comes in multiple forms, including viruses, Trojan horses, logic bombs, worms, scumware, spyware, keystroke loggers and rootkits. The differences between these types of programs may be found in this glossary; however, the end result is often the same.

Man-In-The-Middle Attack

A form of active eavesdropping in which the attacker makes independent connections with the victims and relays their messages between them, making them believe that they are talking directly to each other on a private connection.

Medical Records

Medical records means records which relate to the identification, prevention, cure or alleviation of any disease, illness or injury including psychological disorders, alcoholism and drug addiction.

Mismanagement (See also Corruption, Waste, Fraud, Abuse)

Management that is careless or inefficient.

Mobile code refers to scripting languages used for Internet applications. It is a program, script, macro or other portable instruction that can be shipped unchanged to a variety of platforms and executed with the same result. Some of the most common forms of mobile code are JavaScript, Asynchronous JavaScript and eXtended Markup Language (XML) or AJAX, Java applets, ActiveX, and Flash. Mobile code can be transmitted across the network and downloaded and executed on your computer without explicit installation or permission from you. Shockwave movies and macros embedded in Microsoft office documents are mobile code. Mobile code can also be downloaded through an e-mail attachment. In almost all situations, the user is not aware that the mobile code is downloading and executing on the workstation. Mobile code has been adapted to run on cell phones, PDAs, and other devices.

Modem

(From **mo**dulator-**dem**odulator) is a device that modulates an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded to reproduce the original digital data. Modems can be used over any means of transmitting analog signals, from driven diodes to radio.

N back to top

National Archives and Records Administration
The National Archives and Records Administration (NARA), as an independent federal agency, is America's national record keeper. Its mission is to ensure ready access to the essential evidence that documents the rights of American citizens, the actions of federal officials, and the national experience, and the discovery, use, and knowledge from this documentary heritage.

Need to know

According to the Privacy Act, it pertains to those officers and employees of an agency which maintains the record who have a need for the record in the performance of their duties. (Applies to intra-agency.) Also, a basic Information Assurance principle supporting confidentiality.

National Institute of Standards and Technology (**NIST**)

NIST sets standards for many types of technical performance, including information technology systems and their security. Federal agencies are required to adhere to NIST standards regarding numerous aspects of security for information technology.

Non-Federal Records (Non-Records)

Non-federal records (i.e. non-records) are materials used solely for reference, exhibition or convenience purposes. An individual's personal papers are not federal records even if kept in the office or work area.

Non-repudiation

The ability to determine the identity of a party to an interaction and to ensure that a message came from who it claims to have come from.

O back to top

Office of Management and Budget

The office of Management and Budget's (OMB) predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. OMB has oversight over government Privacy Act implementation. It also has oversight of the development of federal regulations. Further, it oversees federal implementation of the Paperwork Reduction Act.

Office of Personnel Management (OPM) Personnel Records

Office of Personnel Management personnel records means records maintained for the Office of Personnel Management by the Department and used for personnel management programs or processes such as staffing, employment development, retirement, and grievances and appeals.

Original Equipment Manufacturer (OEM)

The original manufacturer of a component for a product, which may be resold by another company.

Open Source Software

Computer software for which the source code and certain other rights normally reserved for copyright holders are provided under a software license that meets the Open Source Definition or that is in the public domain. This permits users to use, change, and improve the software, and to redistribute it in modified or unmodified forms. It is very often developed in a public, collaborative manner. Open source software is the most prominent example of open source development and often compared to user-generated content. The term *open source software* originated as part of a marketing campaign for free software.[1] A report by Standish Group states that adoption of open source software models has resulted in savings of about $60 billion per year to consumers.

P back to top

Packet
A formatted block of data carried by a packet mode computer network.

Paperwork Reduction Act of 1995

The Act, which went into effect October 1, 1995, requires agencies to plan for the development of new collections of information and the extension of ongoing collections well in advance of sending proposals to OMB. Agencies must: seek public comment on proposed collections of information through "60-day notices" in the *Federal Register*; certify to OMB that efforts have been made to reduce the burden of the collection on small businesses, local government, and other small entities; and have in place a process for independent review of information collection requests prior to submission to OMB. Each bureau or office has an Information Collection Clearance Officer which carries out these duties on behalf of the bureau or office.

Patch

Minor updates to programs that are distributed with only the changes and not the whole program. Patches are commonly issued as a fix to a program or to mitigate a security vulnerability.

PDA (Personal Digital Assistant) back to top

The predecessor of a Smartphone, a small, hand-held computer that can store and download information between the device and a computer. PDAs, such as BlackBerrys, Palm Pilots or Pocket PCs, are vulnerable for a number of reasons. Their convenience, portability, low cost, and small size mean they are widely used, easy to steal and difficult to control. They often have wireless capability which is extremely unsecure. PDAs need to be password protected and encrypted. If a PDA is lost or stolen, it needs to be reported as a security incident.

Peer-to-peer Networks (P2P) and Local Shares

You are responsible for knowing what practices are prohibited, and not doing them. Using peer-to-peer file sharing software is an example of a prohibited practice. Peer-to-peer (P2P) file sharing software poses a threat to IT security. Peer-to-Peer refers to any software or system allowing individual users of the Internet to connect to each other and trade files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. Sharing out local folders is also P2P sharing and could transfer infected files between computers without checking for malware.

Just a few of the many peer-to-peer file sharing software products include:

- BitTorrent
- Frostwire
- gtk-gnutella
- FastTrack
- MLDonkey
- Mininova
- isoHunt
- Shareaza

Permissions

Access rights to specific users and groups of users. These systems control the ability of the users affected to view or make changes to the contents of the file system.

Personal Firewall

An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. A personal firewall differs from a conventional firewall in terms of scale. Personal firewalls are typically designed for use by end-users. As a result, a personal firewall will usually protect only the computer on which it is installed. Many personal firewalls are able to control network traffic by prompting the user each time a connection is attempted and adapting security policy accordingly. Personal firewalls may also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted.

Personal Information

Equates to PII or Privacy Information; see below.

Personal papers back to top

Personal papers are documentary materials, or any reasonably segregable portion thereof, of a private or nonpublic character that do not relate to or have any effect upon the conduct of agency business.

Pharming

A hacker attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. DNS servers are computers responsible for resolving Internet names into their real addresses — they are the "signposts" of the Internet. Compromised DNS servers are sometimes referred to as "poisoned".

Phishing

A high-tech scam that uses Internet links sent via e-mail, spam or pop-up messages that look official, to deceive you into disclosing charge card numbers, bank account information, Social Security number, passwords, or other sensitive information or PII. For example, you may receive an e-mail that looks official (from your office, your bank, the IRS, or your charge card company) providing a link and requesting that you type in your Social Security number and other personal information for verification purposes. If you respond to the message, you may later find that someone has purchased a car using your name and credit.

Piggy-backing (or Tailgating)

When a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint. The act may be legal or illegal, authorized or unauthorized, depending on the circumstances. However, the term more often has the connotation of being an illegal or unauthorized act. To describe the act an unauthorized person that follows someone to a restricted area *without* the consent of the authorized person, the term **tailgating** is also used. "Tailgating" implies without consent (similar to a car tailgating another vehicle on the freeway), while "piggybacking" usually implies consent of the authorized person.

PII (Personally Identifiable Information)

A single identifier or combination of personal information that allows an individual to be uniquely identified. PII, as defined by the Office of Management and Budget (OMB) Memo 06-19 of July 12, 2006 is "information which can be used to distinguish or trace an individual's identity such as their name, Social Security number, biometrics records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

Port

An application-specific or process-specific software construct serving as a communications endpoint used by Transport Layer protocols of the Internet Protocol Suite, such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). A specific port is identified by its number, commonly known as the **port number**, the IP address it is associated with, and the protocol used for communication.

Privacy back to top

The right to be left alone and the right to control conditions under which information pertaining to individuals is collected, disseminated and used. The International Association of Privacy Professionals defines Privacy as “The appropriate use of personal information under the circumstances. What is appropriate will depend on context, law, and the individual’s expectations; also, the right of an individual to control the collection, use, and disclosure of personal information.”

Privacy Act of 1974

The Privacy Act (5 U.S.C. 552a) established controls over what personal information the Federal government collects and how it uses or discloses that information. The Privacy Act has four basic objectives: (1) To restrict disclosure of personally identifiable records maintained by agencies; (2) To grant individuals increased rights of access to agency records maintained on them; (3) To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete; and (4) To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Privacy Act Statement

When personally identifiable information is collected directly from an individual, that individual must be provided with a Privacy Act Statement that describes the information collection’s purpose, planned routine uses, the legal authority for the collection, whether providing the information is voluntary or mandatory, and any consequences for not providing the requested information. It can be included on the form (paper or web-based), in a separate handout, or read to the individual.

Privacy Act Warning Notice

A notice (paper or electronic) that informs users of the system of records of the restrictions and the penalties for not abiding by those restrictions (See DOI Privacy Act Warning Notice, 383 DM 8, Illustration 1). These notices must be posted on file folders, cabinets, or other storage devices containing privacy files.

Privacy Impact Assessment (PIA)

The Privacy Impact Assessment is a process used to evaluate the privacy risks of information on individuals in government systems. This is a tool for the system owners and developers to use to assess privacy risks and requirements through the early stages of a systems development or when amendments to a system are made.

Privacy Incident

A privacy incident is the potential loss of control, compromise, unauthorized disclosure, or unauthorized acquisition or access to PII, whether physical or electronic, and includes both suspected and confirmed incidents.

Privacy Information back to top

PII or personal information includes any information linked, or linkable, to a named individual, whether directly named or indirectly inferred. Such information includes the individual's full name, Social Security number, home address, home telephone number, finger and voice prints, birth date, medical, financial and family information, beliefs and affiliations, and any other information that is identifiable to the individual

Privacy Notice

A brief description that informs individuals on what information is collected and how it will be used by the agency. Because the Privacy Notice should serve to notify individuals before they engage with an agency, a Privacy Notice should be provided on the specific webpage or application where individuals have the opportunity to make PII available to the agency.

Privacy Policy

A single, centrally located statement that is accessible from an agency's official homepage. The Privacy Policy is a consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities.

Proprietary Data

Manufactured exclusively by the owner of intellectual property rights (IPR), as with a patent or trade secret.

Protected Information

Information about U.S. citizens and lawful permanent residents that is subject to information privacy, civil rights, and civil liberties protections under the U.S. Constitution and Federal laws of the United States, including, but not limited to, the Privacy Act, the E-Government Act, and the Federal Information Security Management Act (FISMA).

Protocols

Sets of rules and formats that regulate the way data is transmitted between computers.

Proxy

A server (a computer system or an application program) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. A proxy server keeps devices behind it anonymous (mainly for security). A proxy server also speeds access to a resource (via caching). It is commonly used to cache web pages from a web server

Q back to top

QR Codes (Quick Response Codes)

Matrixed barcodes originally developed to be a dense data store for automated data acquisition in the auto industry. This format contains numeric, alpha-numeric, binary and Kanji (due to its invention by a Toyota subsidiary) data. A QR Code reader, often in the form of an application on a smartphone, can read and process the data in those images through the camera.

R back to top

Real Identity Act

Beginning April 21, 2014, national standards for state issued driver's licenses and identification cards used to board commercial aircraft and access federal facilities.

Record

A record according to the Privacy Act is any item, collection, or grouping of information about an individual that is maintained by an agency.

Records Officer

The Department of the Interior Records Officer is responsible for providing leadership and direction for the Department's records management program. The program properly identifies recordkeeping requirements and manages needed records throughout their life cycle.

Records Retention and Disposition Schedules

Schedules that identify various categories of records, and establish the retention period and ultimate disposition for each category. Disposition of the records are either temporary or permanent.

Remote Access

A communication with a data processing facility from a remote location or facility through a data link.

Risk

The likelihood that a particular threat source will exploit or trigger a particular information system vulnerability, and the resulting impact if this should occur.

Role-Based Access Control (RBAC) back to top

An approach to restricting system access to authorized users. It is a newer alternative approach to mandatory access control (MAC) and discretionary access control (DAC). RBAC is sometimes referred to as role-based security.

Rootkit

A program (or combination of programs) designed to take fundamental control (in Unix terms: "root" access, in Windows: "Administrator" access) of a computer system without authorization by the system's owners and legitimate system administrators.

Routine Use

A use of a record for a purpose which is compatible with the purpose for which it was collected (these are identified in the Privacy Act system of records notice published in the *Federal Register*). It is important the agency employees comply with the limits of the routine uses.

Rules of Behavior (ROB)

Rules of Behavior are a set of rules for computer usage for individual users of the DOI network, DOI computers, and DOI Information Systems. These rules clearly delineate responsibilities of and expectations for all individuals with access to the system. The rules are consistent with DOI IT policy and are as stringent as necessary to provide adequate security. The rules cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. The rules reflect technical security controls in the system. For example, rules regarding password use are consistent with technical password features in the system.

S back to top

Scam

Confidence tricks exploit typical human qualities like greed, dishonesty, vanity, honesty, compassion, or a naïve expectation of good faith on the part of the con artist. Just as there is no typical profile for swindlers, neither is there one for their victims. Virtually anyone can fall prey to fraudulent crimes. Certainly, victims may possess a level of greed which exceeds their caution as well as a willingness to believe what they want to believe. However, not all fraud victims are greedy, risk-taking, self-deceptive individuals looking to make a quick dollar. Nor are they all naïve or uneducated.

Scans

The use of a computer program to map systems to identify weaknesses in applications, computers or networks. Step 1, typically the scanner will first look for active IP addresses, open ports, Operating Systems and any applications running. Step 2, try to determine the patch level of the OS or applications. In this process the scanner can cause an exploit of the vulnerability such as crash the OS or application. Step 3, the final phase the scanner may attempt to exploit the vulnerability.

Script (Scripting Language, **Script Language** or **Extension language)** back to top

A programming language that allows control of one or more software applications. "Scripts" are distinct from the core code of the application, which is usually written in a different language, and are often created or at least modified by the end-user. Scripts are often interpreted from source code or bytecode, whereas the applications they control are traditionally compiled to native machine code. Scripting languages are nearly always embedded in the applications they control. The name "script" is derived from the written script of the performing arts, in which dialogue is set down to be spoken by human actors. Early script languages were often called *batch languages* or *job control languages*. Such early scripting languages were created to shorten the traditional edit-compile-link-run process. An example many people have used is a web browser like Firefox. Firefox is written in C/C++ and can be controlled by JavaScript.

Scumware

Any program that gets on a computer from Internet sites without consent, and often without knowledge.

Search Engine Optimization (SEO)

The process of improving the visibility of a website or a web page in search engines. In general, the higher and more frequently a site appears in the search results list, the more visitors it will receive from the search engine's users.

Security Event

Any observable occurrence on a network or system. Events include a user connecting to a file share, a server receiving a request for a Web page, a user sending electronic mail (email), and a firewall blocking a connection attempt. *Adverse events* are events with a negative consequence, such as system crashes, network packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malicious code that destroys data.

Security Groups

Lists of computer accounts which are authorized to have file permissions to specific folders or directories.

Security Incident

An incident can be thought of as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. It may involve denial of service, malicious code, unauthorized access, or inappropriate usage. [NIST SP 800-61]

Senior Agency Official for Privacy (SAOP)

OMB requires that each agency designate an SAOP for that agency. At the Department of the Interior, the Chief Information Officer is designated as the SAOP.

Sensitive But Unclassified (SBU) back to top

A designation of information that, though not classified as “Secret” or “Top Secret”, often requires strict controls over its distribution.

Sensitive Data

Any information not explicitly classified where the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act. Personally Identifiable Information and Privacy Act data are considered sensitive data.

Sensitive Data Extracts

Elaborated on by OMB Memorandum 06-16 issued June 23, 2006 after the Veterans Administration breach of names and social security numbers. http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf The document detailed the treatment of sensitive data stating that extracting data from sensitive databases must be logged, and tracked so it can be deleted after 90 days if not still being used.

SHA (Secure Hash Algorithm)

A set of cryptographic hash functions designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. The three SHA algorithms are structured differently and are distinguished as *SHA-0*, *SHA-1*, and *SHA-2*. The *SHA-2* family uses an identical algorithm with a variable digest size which is distinguished as *SHA-224*, *SHA-256*, *SHA-384*, and *SHA-512*. SHA-1 is the best established of the existing SHA hash functions, and is employed in several widely used security applications and protocols. In 2005, security flaws were identified in SHA-1, namely that a possible mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although no attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives.

Shareware

Proprietary software that is provided to users without payment on a trial basis and is often limited by any combination of functionality, availability or convenience. Shareware is often offered as a download from an Internet website or as a compact disc included with a periodical such as a newspaper or magazine. The aim of shareware is to give buyers the opportunity to use the program and judge its usefulness before purchasing a license for the full version of the software.

Signature

A malware signature is the machine code or the behavior of the file. When antivirus software scans a file for viruses, it checks the contents or behavior of a file against a dictionary of virus signatures. If a virus signature is found, the antivirus software can resort to some combination of quarantine, repair or deletion.

Smartphone back to top

A smartphone combines the functions of a personal digital assistant (PDA) and a mobile phone.

Social Engineering

This term is used to describe techniques that rely on psychology, or human nature, to trick people into revealing passwords and other information that hackers can use to compromise system security. Attackers will try social engineering techniques that may use bullying, cajoling, being very friendly, intimidating or shaming you into providing information they are not authorized to know. Never give your password to anyone; not your supervisor, not the help desk, not a system administrator. If someone claiming to be the police, FBI, or from the IG's office wants your password, ask them to go through your supervisor or BCISO. Protecting your password is the first line of defense in safeguarding computer networks and should never be given to anyone. No legitimate authority will ask for your password without being willing to get a subpoena. Protecting passwords is a serious issue.

Social Networking

Online communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services.

Software Development Life Cycle (see System Development Life Cycle)

Software Piracy

The unauthorized use of material that is covered by copyright law, in a manner that violates one of the copyright owner's exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works. For electronic and audio-visual media, unauthorized reproduction and distribution is also commonly referred to as *piracy***.** An example is the unlawful downloading of copyrighted material and sharing of recorded music over the Internet in the form of MP3 files is more prominent now than since before the advent of the Internet or the invention of MP3 files, even after the demise of Napster and a series of infringement suits brought by the RIAA.

Spam

Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.

Spyware

A type of malware that is surreptitiously installed on computers and that collects information about users without their informed consent. The presence of spyware is typically hidden from the user. Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spyware such as keyloggers is installed by the owner of a shared, corporate, or public computer on purpose in order to monitor users.

Spoofing back to top

Forging an e-mail header to make it appear as if it came from somewhere or someone other than the actual source. A spoofed URL describes one website that poses as another legitimate website.

Statistical Records

Statistical records are records in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual.

System Development Life Cycle (SDLC)

The systems development life cycle (SDLC) is a conceptual model used in project management that describes the stages involved in an information system development project, from an initial feasibility study through maintenance of the completed application.

Various SDLC methodologies have been developed to guide the processes involved, including the waterfall model (which was the original SDLC method); rapid application development (RAD); joint application development (JAD); the fountain model; the spiral model; build and fix; and synchronize-and-stabilize. In general, an SDLC methodology follows the following steps:

1. The existing system is evaluated. Deficiencies are identified. This can be done by interviewing users of the system and consulting with support personnel.
2. The new system requirements are defined. In particular, the deficiencies in the existing system must be addressed with specific proposals for improvement.
3. The proposed system is designed. Plans are laid out concerning the physical construction, hardware, operating systems, programming, communications, and security issues.
4. The new system is developed. The new components and programs must be obtained and installed. Users of the system must be trained in its use, and all aspects of performance must be tested. If necessary, adjustments must be made at this stage.
5. The system is put into use. This can be done in various ways. The new system can phased in, according to application or location, and the old system gradually replaced. In some cases, it may be more cost-effective to shut down the old system and implement the new system all at once.
6. Once the new system is up and running for a while, it should be exhaustively evaluated. Maintenance must be kept up rigorously at all times. Users of the system should be kept up-to-date concerning the latest modifications and procedures.

System Guidelines

System guidelines are a set of formal, written instructions to employees working with a system of records. They contain operating procedures to be followed in maintaining a specific records system and supplement the Department's regulations and directives pertaining to the Privacy Act and any bureau directives which apply generally to all of its systems of records subject to the Act.

System Manager back to top

The DOI regulations refer to a "System Manager" as the official designated in a system notice as having the administrative responsibility for a system of records.

System of Records

A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual (also referred to as a “Privacy Act System”).

System of Records Notice (SORN)

A Privacy Act notice that is published in the Federal Register for all collections of information on individuals where the information is retrieved by a name or other personal identifier.

System Security Plan (SSP)

The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the senior agency information security officer (SAISO).

T back to top

Tablet Computer

A tablet computer, or simply tablet, is a complete mobile computer, larger than a mobile phone or personal digital assistant, integrated into a flat touch screen and primarily operated by touching the screen. It often uses an onscreen virtual keyboard or a digital pen rather than a physical keyboard.

Telework

A term referring to substituting telecommunications for any form of work-related travel.

Terrorism Information

Any information collected, produced, or distributed by intelligence, law enforcement, military, or homeland security relating to transnational terrorism; threats posed by such groups or individuals to the United States, United States persons, United States interests, or to those of other nations; communications of or by such groups or individuals; or groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Thin Client back to top

A client computer or client software in client-server architecture networks which depends primarily on the central server for processing activities, and mainly focuses on conveying input and output between the user and the remote server. In contrast, a thick or fat client does as much client processing as possible and passes only data for communications and storage to the server.

Third party

A third party is someone other than the subject of the file.

Third-party websites or applications - The term "third-party websites or applications" refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website.

Threat

A circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity or availability. Threats exist due to the very existence of an IT environment and not because of any specific vulnerability or weakness.

Trademark

A distinctive sign or indicator used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities. It is a type of intellectual property, and typically a name, word, phrase, logo, symbol, design, image, or a combination of these elements.

Transitory Federal Records

Records that contain information directly related to the Department's mission, operations, and activities, but they are of short term interest (under 180 days) and have minimal or no documentary or evidentiary value.

Trojan or Trojan Horse

A term coined by former MIT-hacker turned NSA employee Dan Edwards. A malicious, security-breaking program disguised as something benign, such as a directory lister, archiver, game, or — in one notorious 1990 case on the Mac — a program purported to find and destroy viruses.

Two Factor Authentication

An authentication factor is a piece of information and process used to authenticate or verify the identity of a person or other entity requesting access under security constraints. **Two-factor authentication (T-FA)** is a system wherein two different factors are used in conjunction to authenticate. Using two factors as opposed to one factor generally delivers a higher level of authentication assurance.

U back to top

USGCB (United States Government Configuration Baseline)

The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration (FDCC) mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain effective configuration settings focusing primarily on security.

United States Code (USC)

The United States Code is the codification by subject matter of the general and permanent laws of the United States. It is divided by broad subjects into 50 titles and published by the Office of the Law Revision Counsel of the U.S. House of Representatives.

URL (Uniform Resource Locator)

An address that specifies the location of a file on the Internet (for example http://www.doi.gov)

V back to top

Virtual Private Network (VPN)

A computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger networks (such as the Internet), as opposed to running across a single private network.

Virus

A virus is a piece of code that can attach itself to other programs but cannot run on its own. It can only execute when the host program is run, and then it is able to attach itself to other programs and replicate. A virus has the potential to slow down the IT system, modify data, or destroy data.

Vulnerability

Absence or weakness of a security control.

W back to top

Waste

The extravagant, careless, or needless expenditure of government funds or the consumption of government property that results from deficient practices, systems, controls or decisions. The term also includes improper practices not involving prosecutable fraud.

Web 2.0

Web development and web design that facilitates interactive information sharing, interoperability, user-centered design and collaboration on the World Wide Web. Examples of Web 2.0 include web-based communities, hosted services, web applications, social-networking sites, video-sharing sites, wikis, blogs, mashups and folksonomies. A Web 2.0 site allows its users to interact with other users or to change website content, in contrast to non-interactive websites where users are limited to the passive viewing of information that is provided to them.

Web Conferencing

Used to conduct live meetings, training, or presentations via the Internet. In a web conference, each participant sits at his or her own computer and is connected to other participants via the internet.

Wi-Fi

A trademark of the Wi-Fi Alliance for certified products based on the IEEE 802.11 standards. This certification warrants interoperability between different wireless devices.

Wireless

Refers to any system of transmitters and receivers that sends radio signals over the air, such as a Wi-Fi local network, cellular network, or satellite network.

WEP (Wired Equivalent Privacy)

A wireless network security standard encrypting data over radio waves. It is obsolete since it is very insecure and does not offer end-to-end security.

WPA2 (Wi-Fi Protected Access)

A certification program to indicate compliance with the security protocol created by the Wi-Fi Alliance created in response to weaknesses found in WEP.

Worms back to top

A worm is a fully independent program that can copy itself from one computer to another, usually via a network. Worms primarily cause damage by slowing down the IT system.

Written consent

Written consent is provided by the subject of the file to release information from the subject's file.

Z back to top

Zombie

A computer that has robot (bot) software installed and is under the control of a bot-herder.